VULNERABLE UNIVERSITY

ABHISHEK BIRDAWADE | SRUSHTI DESHPANDE | VAIBHAV WAGH

GAYATRI BEDRE

Introduction

Cyber Security is method of protecting and securing the computer devices, network and program from cyber-attack. The importance of cyber security is rising. Cyber criminals are more sophisticated, changing the attacking approach and they are creating a really crucial conditions for organizations by affecting their image.

An application vulnerability means lack of security or weakness in an application that cause a major issue. This happens due to not validating inputs, flaws in application design and misconfigured servers. Cyber security is a vast field and immerging daily. With increasing digital theft and cyber criminals, we need security tester and practioners to help us tackle the increasing problem. It is necessary for them to learn testing without violating cyber laws. The vulnerable web application will provide a platform to learn and test their skills in their own local environment.

Developers, security auditors, and penetration testers can utilize the vulnerable web apps to test the many hacking tools and offensive approaches available at any time, as well as to exercise their knowledge and abilities during training sessions (and especially after). preparing for their upcoming opportunities.

Intentionally Vulnerable web-applications for testing can help security professionals for hacking, on their local system, they engage in offensive and defensive operations that imitate real-world web environments. Security professionals can practice and enhance their skills regarding web-application security testing by learning and practicing about various technical and non-technical bugs and vulnerabilities.

Rationale

Vulnerable university can help professional hackers to brush up their skills. That would help to find the vulnerabilities more efficiently and improve the performance of the application. The professional hackers can get a lot of types of vulnerabilities on a single platform.

Objective

1. To identify the threats in the web application, servers & websites.
2. To find potential vulnerabilities of the system and try to resolve those vulnerabilities.
3. To help in detecting to every possible security risk in the system.
4. Examine the impact occurs due to vulnerabilities.
5. To help the organizations and developer teams to resolving the security problem.
6. Improve the skills of the security professionals.
7. Introducing the various kind of hacking techniques without violating cyber laws.
8. Provide cyber education to students regarding technical and non-technical vulnerabilities.

Methodology/Planning for Project

Vulnerable university is a single platform that is developed for security professionals to enhance and practice their skills.

1)Vulnerabilities Collection: We collected most of the common vulnerabilities both technical and non-technical & gathered the knowledge of how the vulnerabilities can be introduced in a web application and the PHP server.

2)Website designing: After listing the vulnerabilities we prepared how we can make our server and web application vulnerable to those vulnerabilities which the student can reproduce locally.

3)Creating the frontend: Then we created the vulnerable frontend interface of the website which the students can interact with and practice testing the vulnerabilities.

4)Creating the backend: After creating frontend of the platform, we created the backend of the application using PHP server which is intentionally vulnerable and cable of being deployed locally on any machine.

5)API middleware: After the frontend and backend both being created, we used APIs to connect them together using RESTful APIs, which also are vulnerable to CRUD related vulnerabilities and various other vulnerabilities.

6)Docker container: After creating the intentionally vulnerable university's web application with backend, we stacked it together in a docker container so that the student can easily deploy and run the web-application & start testing/practicing their hacking skills for good.

Expected Outcome

Input: Intentionally vulnerable university web-application with frontend website and backend server and APIs connecting them.

Expected Output: Students will be able to test their hacking skills on their individual local environment.

Actual Output: Students are able to practice finding technical and non-technical web-application vulnerabilities in their local environment.